



Компьютерные вирусы и защита от них

Выполнил ученик
10 «М» класса
Вилков Артем

Основное понятие компьютерного вируса

- ▶ Подводя итог можем сказать что компьютерный вирус это программа нарушающая действие системы.
- ▶ Есть вирусы разных сложностей и направленностей
- ▶ Так же отличаются по мере самовоспроизведения
- ▶ Может независимо от желания пользователя нарушать работу системы из-за ошибки или совокупности ошибок в программном коде.

Трояны

- ▶ Троян или троянский конь — программа попадающая в устройство благодаря неопытности пользователя.
- ▶ Сейчас рассмотрим такой пример на базе Windows XP (Oracle VirtualBox).
- ▶ Как мы можем видеть, после запуска .bat файла наш смоделированный Windows перестал работать и требует ввод специального кода.
- ▶ Благо, пароль я уже знаю и могу спокойно продолжить работу

AdWare

- ▶ Программы данного типа предназначены для показа рекламы
- ▶ В наше время чаще всего встречаются в виде расширения для браузера которое не так то просто удалить.
- ▶ Иногда приходится редактировать реестр чтобы полностью избавиться от данной программы
- ▶ Чаще всего пользователя настолько раздражает назойливая реклама что он предпринимает решение переустановки ОС

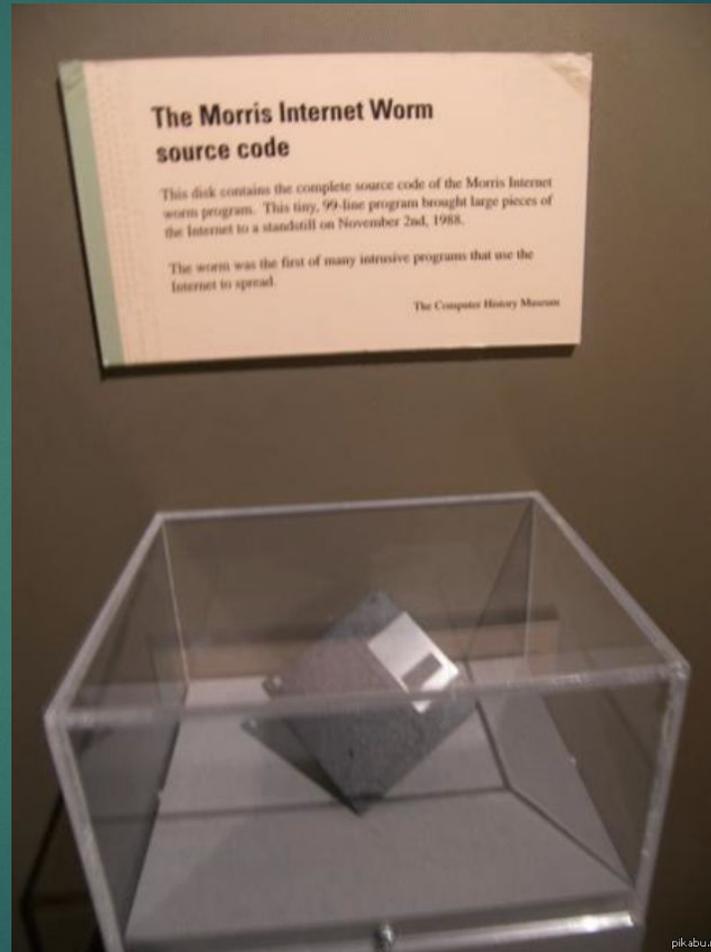


УПАКОВЩИКИ

- ▶ Часто является хорошо скрытым трояном
- ▶ Есть 3 типа упаковщиков, подозрительные, многократные, редко используемые
- ▶ Выделить упаковщики в отдельный класс, потому что они совпадают с троянами

Червь Морриса

- Открыт 2 ноября 1988 года
- Получил огромную известности благодаря СМИ
- Запускателем червя был обычный студент
- Ущерб около \$96 млн



АНТИВИРУСЫ

- ▶ Условно делятся на серверные, скрипы, SaaS сервисы
- ▶ Существует специальный антивирус от слежки спецслужб
- ▶ Существуют лжеантивирусы которые являются не честным источником добычи прибыли
- ▶ Существует некая база антивирусов, представляет из себя справочник со всеми вирусами

DDoS и DoS атаки

- ▶ DoS от англ. Denial of Service — отказ в обслуживании
- ▶ Юридически факт атаки очень сложно доказать
- ▶ Все DoS атаки «поедают» ресурсы компьютера.
- ▶ Всего их 4 типа, и большая часть атак совершается «шутки ради» или из-за личной неприязни

Основные жертвы DoS атак



Защита от DoS атак

- ▶ Никогда не давайте свой IP-адрес кому попало
- ▶ ВСЕ сетевые сервисы должны быть защищены брандмауэром
- ▶ Программное обеспечение, которое установлено на сервере, должно быть в актуальном состоянии, а именно: должно быть установлено последнее ПО, касающееся обеспечения безопасности системы.
- ▶ Если же на вас все таки удалось напасть то стоит сменить IP адрес, тогда злоумышленникам будет труднее вас достать. А иногда спасает динамический IP или VPN соединение.